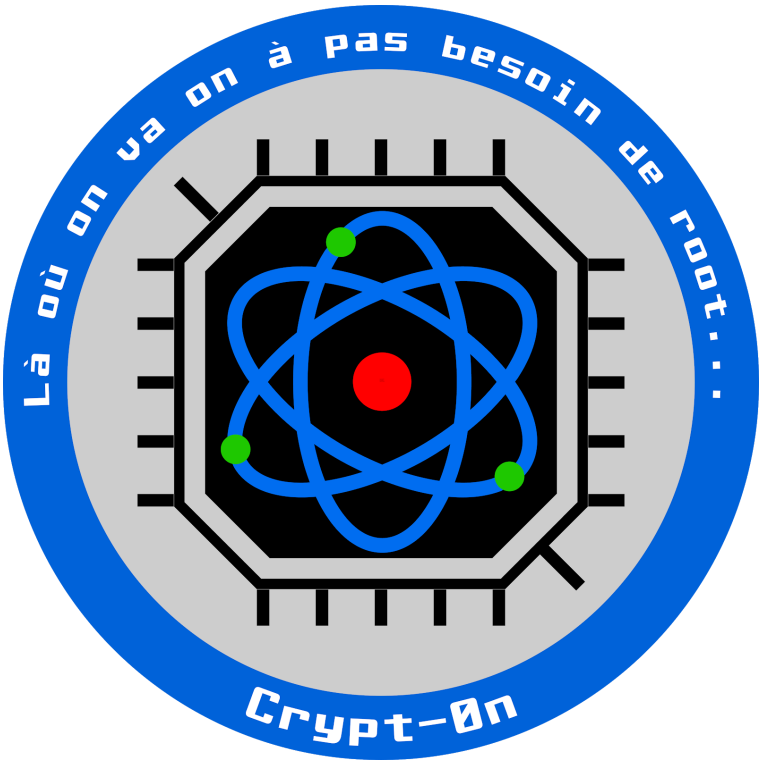

Fiche Malware

HOUDINI (H-WORM)

Version 1.0
Date : 03/04/2018

TLP:WHITE

Crypt-0n
https://www.crypt-0n.fr

Décharge de responsabilité

Ce document est mis à disposition par l'association Crypt-0n ***uniquement à titre informatif et à des fins pédagogique****. Les informations qu'il contient sont publié "en l'état" sans aucune sorte de garantie ni expresse ni implicite. Les informations contenu dans ce document peuvent êtres mis à jour sans préavis.*

Crypt-0n décline toute responsabilité pour les éventuelles erreurs ou omission figurant dans ce document.

Sommaire

Sommaire **3**

Le Malware **4**

Description 4

Fonctionnalités du Malware 4

L’installation 5

Propagation 5

Communications réseau 5

Détection antivirus 6

Conclusion 6

Nettoyages des postes **7**

Détecter le Malware 7

Supprimer le Malware 7

Intégrité des données 7

Préconisation post infection **8**

Les postes 8

Les périphériques de stockage 8

Le Malware

Description

Le malware analysé est connu sous le nom de “Houdini” ou “H-worm”.
Ce malware se présente sous la forme de script VBScript. Il existe également d’autres variantes (fichier wsf, Windows Script File qui permet d’intégrer des scripts VBScript).
Ce malware permet d’exfiltrer des données via le « useragent » et d’exécuter des commandes et/ou des programmes.

Fonctionnalités du Malware

Interface de la console du C&C

Les différentes fonctionnalités du malware sont les suivantes :

- Exécuter du code VBS envoyé par le C&C
- Mise à jour du malware
- Désinstallation du malware
- Téléchargement d’un fichier depuis le serveur
- Téléchargement d’un fichier depuis un site web
- Exfiltration de fichier sur le C&C
- Envoi d’information sur les disques de la victime au serveur C&C
- Envoi de la liste des fichiers/dossiers d’un répertoire au C&C
- Envoi de la liste des processus au C&C
- Exécution de commande et envoi du résultat au C&C
- Suppression d’un fichier/dossier
- Arrêter un processus
- Configuration du temps entre les différentes communications

L’installation

Le malware s’installe dans le répertoire %temp% du contexte de l’utilisateur
La persistance du malware est réalisé via une copie du malware dans :

- `%USERPROFILE%\Start Menu\Programs\Startup\{malware file name}`

Le malware tente également de s’inscrire dans le registre dans les clés « run » dans les ruches HKLM et HKCU :

- `HKEY_CURRENT_USER\software\microsoft\windows\currentversion\run\`
  - clé : `{malware file name}`
  - valeur : `"wscript.exe //B "%temp%\{malware file name}"`
- `HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\run\`
  - clé : `{malware file name}`
  - valeur : `"wscript.exe //B "%temp%\{malware file name}"`

A la première installation, le malware va tenter de créer l’entrée de registre suivante :

- `HKEY_LOCAL_MACHINE\SOFTWARE\{malware file name}`

Il va ensuite dans cette entrée ajouter une clé « **Default** » avec la valeur « **True** » ou « **False** » s’il a été exécuté depuis un périphérique USB ainsi que la date de première exécution (exemple : « true – DateDinstallation » ou « false – DateDinstallation »).

Propagation

A chaque exécution du malware, celui-ci se propage sur tous les lecteurs connectés au poste.

La propagation est réalisée via une copie du malware sur les disques connectés au poste infecté, puis en créant des raccourcis portant les noms des fichiers présents sur les disques et pointant sur la copie du malware présent sur le disque.

Communications réseau

Les communications réseau sont réalisées en HTTP via requêtes **GET** et **POST**, les communications sont en règle général réalisé sur les ports « exotiques » (diffèrent de 80, mais peut quand même être utilisé).

Il est possible d’identifier ces communications en recherchant dans les URL les valeurs suivantes :

- `*/is-enum-driver`

- `*/is-enum-faf`
- `*/is-enum-process`
- `*/is-cmd-shell`
- `*/is-ready`
- `*/is-sending`
- `*/is-recving`

Le « useragent » utilisé n'est pas commun, en effet il est possible de retrouver des informations sur le poste, les différents champs présents dans le « useragent » sont séparer par le délimiteur suivant : **<** | **>**

Détection antivirus

De nombreuses variantes de ce malware sont détectées, mais il est très simple d'offusquer le code, car le malware est un script VBScript.

Afin de s'assurer de la détection de chaque souche de ce malware, il est donc nécessaire de soumettre toutes les souches identifiées aux différents éditeurs antivirus.

Conclusion

Ce malware est très simple à mettre en place et à rendre indétectable par les antivirus grâce à son format facilement obfuscable, mais il est du coup facilement désobfuscable.

Il est également très volatile, car se duplique automatique sur tous les disques connectés au poste infecté.

Les données qui transitent entre le poste infecté et le C&C ne sont pas chiffrées et les connexions sont facilement identifiables.

Le principal risque est l'envoi et l'exécution d'un programme tiers (virus, hacktool, etc…) sur le poste déjà infecté.

/!\ Attention, il existe d'autres variantes à ce malware qui utilisent d'autres séparateurs dans le « useragent » ainsi que d'autres requêtes http pour l'envoi et réception d'instructions au C&C.

Nettoyages des postes

Détecter le Malware

Il est possible de détecter facilement la présence de ce malware dans les logs proxy de navigation en recherchant le séparateur utilisé dans le « useragent » (`<|>`) ou certaines chaines de caractère dans les URL (`/is-ready`).

Pour plus d'information, voir la partie « Communications réseau » dans la première partie de ce document.

Supprimer le Malware

Il est possible de nettoyer assez facilement les postes infectés en supprimant le malware de la racine du disque, de chaque dossier **%temp%** et **startup** de chaque utilisateur ainsi que de supprimer les entrées de registre dans les ruches **HKLM** et **HKU**.

Pour plus d'information, voir la partie « L'installation » dans la première partie de ce document.

Intégrité des données

Afin de pouvoir garantir l'intégrité des données du poste, il est nécessaire que le poste infecté ne se soit jamais connecté à internet depuis un autre réseau que celui de l'entreprise et que depuis le début de l'infection de poste les requêtes HTTP soient bloquées par le proxy.

Préconisation post infection

Les postes

Nous préconisons la réinstallation complète de chaque poste infecté sans récupération de données pour les postes qui ont été connectés hors SI et/ou qui ont réussi à contacter le C&C (voir dans les logs Proxy web).

Il nous paraît intéressant de faire un rappel à l'utilisateur sur l'utilisation des périphériques USB dans l'entreprise voire même faire bloquer les périphériques de stockage sur son poste.

Les périphériques de stockage

Il est nécessaire de voir avec l'utilisateur pour connaître tous les périphériques de stockage qui ont été connectés au poste compromis afin de pouvoir les faire formater.